Department of Homeland Security Daily Open Source Infrastructure Report for 24 August 2005

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- Vnunet reports the Anti−Phishing Working Group warns phishers are becoming more sophisticated with the development of malicious crimeware software that can bypass conventional IT security systems and steal identity information for financial crime. (See item 4)
- The New York Metropolitan Transportation Authority has announced plans for a $200 million security system for the city's sprawling subway, bus network, and two major commuter rail lines, featuring closed−circuit cameras and motion detectors. (See item 8)
- The Associated Press reports an inquiry is being launched into why a New York state−run water playground may have spread more than 2,000 cases of gastrointestinal illnesses. (See item 20)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *August 23, The Arizona Republic* — **Palo Verde reactor shut down for tests.** With one Palo Verde reactor out of service for maintenance, operators of the nation's largest nuclear power plant shut down a second reactor Monday, August 22, to complete required software tests.

Arizona Public Service Co. (APS) said it expected to finish the tests and return Unit II to full power by the end of the week. Palo Verde Unit I, shut off since August 12, should be back in service in a few days. Although it's rare to have two units out, APS said there is still plenty of power for the Phoenix area. Palo Verde nuclear power plant is located near Wintersburg, AZ.
Source: http://www.azcentral.com/news/articles/0823B1−newsupdate23.h tml

[Return to top]

Chemical Industry and Hazardous Materials Sector

2. *August 23, NBC5i (TX)* — **Truck overturns, spilling acid and causing traffic delays in Texas.** A tanker truck filled with sulfuric acid fell on its side late Monday night, August 21, in north Fort Worth, TX, stalling traffic near the Interstate 35W−Highway 287 split. Hazmat crews said there was no danger to drivers; crews cleaned up the mess and moved the truck. The accident happened on southbound I−35W at the Highway 287 northbound ramp. The 18−wheeler was up−righted and lanes were clear on the freeway by 8 a.m. Tuesday, August 23.
Source: http://www.nbc5i.com/news/4885026/detail.html

[Return to top]

Defense Industrial Base Sector

Nothing to report.
[Return to top]

Banking and Finance Sector

3. *August 23, TechWeb News* — **Banks abandoning security feature on home page log−ins.** Some of the biggest banks have abandoned the practice of posting their online account log−in screens on Secure Socket Layer (SSL)−protected pages in an effort to boost page response time and guide users to more memorable URLs, a UK Web performance firm said Tuesday, August 23. Netcraft noted that three of the largest banks in the U.S. now display their log−in forms on home pages not locked down with SSL. According to Netcraft, companies are increasingly hesitant to use SSL's "https" on busy home pages, because SSL slows response time, and consumers prefer easy to−remember URLs. The username and password are still encrypted when sent to the bank's server after the user hits the Submit or Log−in button. However, as Netcraft noted, Microsoft took the practice to task as long ago as April, when in an entry on the developer's official Internet Explorer blog, program manager Eric Lawrence wrote that the idea was flawed and could be exploited by "man−in−the−middle" attacks. In particular, keyloggers could conceivably "leak" characters to another server as they're typed into a non−SSL log−in form before the Submit or Log−in button's clicked.
Source: http://www.techweb.com/wire/security/169600256

4. *August 23, Vnunet* — **Crimeware epidemic spreading fast.** Phishers are rapidly becoming more sophisticated with the development of malicious crimeware software that can bypass conventional IT security systems and steal identity information for financial crime, the

Anti−Phishing Working Group (APWG) warned on Tuesday, August 23. In July 2005, APWG researchers found that phishers are designing systems specifically to neutralize the counter−phishing technologies being deployed by financial institutions and ecommerce sites. APWG researchers reported a marked increase in screenscraper technology by phishers. This shift aims to counter the graphical keyboard systems some financial services firms are using to avoid the hazards of keylogging Trojans that phishers have been using to mine the usernames and passwords directly from the keyboard entry of alphanumerics and symbols. When the user mouseclicks a character on the graphical keyboard, the screenscraper takes a snapshot of the screen and sends it to the phishers' server for inspection, according to APWG researchers. "Crimeware continues to evolve as we have seen the deployment of advanced techniques to steal information. These Trojan horses are moving beyond keylogging and now capture screenshots to obtain end−user credentials," said Dan Hubbard, senior director of security for security firm Websense and APWG analyst.
APWG July Report: http://antiphishing.org/APWG_Phishing_Activity_Report_Jul_05 .pdf
Source: http://www.vnunet.com/vnunet/news/2141436/crimeware−epidemic −takes−hold

5. *August 22, TechWeb News* — **Over 90 percent of companies regularly expose personal information.** According to the second monthly Insider Threat Index generated by security firm Reconnex, a Mountain View, CA−based enterprise risk management vendor, 91 percent of the companies undergoing assessment in July exposed credit card numbers, and 82 percent exposed employee Social Security numbers. "The origin of the vast majority of these disclosures stemmed from human resources departments," according to Reconnex's July index report. "[These departments] often accidentally exposed employees' personal information when they communicate with partners in health insurance, payroll, workers compensation, and other third−party processors," stated the report. In other cases, claimed Reconnex, employees are exposing data by sending files using Web e−mail services such as Hotmail and Yahoo Mail."
Insider Threat Index: http://www.reconnex.net/Threat/
Source: http://www.techweb.com/wire/security/169500283

6. *August 22, Department of Justice* — **Federal racketeering indictments target international smuggling, counterfeit currency operation.** The Department of Justice and the Department of Homeland Security announced on Monday, August 22, that 87 individuals have been indicted and 59 people have been arrested on charges related to international conspiracies to launder money and smuggle counterfeit U.S. currency, weapons, drugs and cigarettes into the United States. The arrests were the result of two parallel undercover law enforcement operations. The FBI undercover operation, Operation Royal Charm, revealed that the illicit organization smuggled highly deceptive counterfeit U.S. currency, manufactured in a foreign country, into the United States on container ships with false bills of lading for toys, rattan furniture and other goods. The indictments allege that in October 2004, a container loaded with approximately $338,000 in counterfeit currency arrived in Newark, followed by a shipment of nearly $3 million in counterfeit currency in December 2004. A third shipment of nearly $2 million in counterfeit U.S. currency was ordered from the subjects. The containers were allegedly sent by defendants after extensive meetings with FBI undercover agents.
Source: http://www.justice.gov/opa/pr/2005/August/05_crm_426.htm

[Return to top]

Transportation and Border Security Sector

7. *August 23, Detroit Free Press (MI)* — **Northwest's strike toll: 1,200 jobs gone.** About 1,200 union jobs have been eliminated since mechanics and plane cleaners walked off the job three days ago, Northwest Airlines said Monday, August 22, as it uses the strike to impose many of the cost−cutting changes it demanded during months of contract negotiations. Northwest has closed 29 of 32 maintenance bases at airports across the country −− all except Detroit, Minneapolis, and Milwaukee. Spokesperson Kurt Ebenhoch said independent companies, with less expensive nonunion workers, have been hired to fix planes at those airports and to clean its planes at every airport. That eliminates the jobs of about 400 mechanics and 800 plane cleaners, who are among the 4,400 members of the Aircraft Mechanics Fraternal Association (AMFA) walking picket lines. Northwest is facing bankruptcy this fall if it keeps losing $4 million a day because of high labor costs, soaring fuel bills and tough competition that limits how much it can charge for tickets. Before the strike, Northwest told AMFA it must reduce the cost of cleaning and fixing its planes by $176 million a year. Hiring outside contractors to do much more of that work is a big part of the airline's plan to do that. A 25% pay cut for all AMFA workers is another.
   Source: http://www.freep.com/money/business/nwa−bar123e_20050823.htm

8. *August 23, Associated Press* — **NYC transit unveils security plans.** The New York Metropolitan Transportation Authority (MTA) announced plans Tuesday, August 23, for a $200 million security system for the city's sprawling subway and bus network and two major commuter rail lines, featuring closed−circuit cameras and motion detectors. The MTA announcement comes six weeks after the terrorist attack on the London subway system that killed 52 people. The security system will cover platforms, stations and terminals but will not be installed inside train cars or buses. Installation of the first cameras was starting Tuesday and the whole system, whose coverage will include bridges and tunnels, should be installed within three years, said MTA Executive Director Katherine Lapp. It is the MTA's largest financial commitment to its counterterrorism program. Although the agency approved a $591 million security plan in 2002, it had spent only a fraction of that sum until this deal with Lockheed Martin. In addition to subways and bus lines, the system will serve the Long Island Rail Road and Metro−North Railroad commuter lines.
   MTA Website: http://www.mta.nyc.ny.us/
   Source: http://www.newsday.com/news/nationworld/nation/wire/sns−ap−nyc−transit−security,0,5538884.story?coll=sns−ap−nation−headl ines

9. *August 23, Associated Press* — **Northwest flight diverted to Honolulu due to mechanical problems.** A Northwest Airlines flight from Seattle to Maui was diverted to Honolulu International Airport over the weekend after a gauge showed loss of oil, a union official said. The Kahului−bound plane landed in Honolulu on Saturday shortly after 6 p.m., Hawaii Department of Transportation spokesperson Scott Ishikawa said. All 230 passengers slept in a conference room at the airport because no available hotel rooms could be found, Ishikawa said. Hal Myers of the Air Line Pilots Association said the pilots in Flight 95 had to throttle the engine back to idle, meaning the two−engine 757 had to make the rest of the trip on power from just one engine. Myers, a veteran pilot himself, said he's had two engine failures during his career. He said this type of incident would go relatively unnoticed if Northwest wasn't under scrutiny because of the strike by mechanics.

Source: http://www.usatoday.com/travel/flights/2005−08−23−nwa−mechan ics_x.htm

10. *August 23, Department of Transportation* — **Transportation Secretary Mineta announces $80 million in emergency funds to repair damaged roads in 18 states.** Department of Transportation (DOT) Secretary Norman Y. Mineta on Tuesday, August 23, approved $80 million in emergency relief funds for 18 states and U.S. territories to repair roads and bridges damaged by recent flooding, storms or other catastrophic events. The Department's Federal Highway Administration will reimburse states for costs associated with reconstructing or replacing damaged highways and bridges, establishing detours, removing debris, and replacing signs, lighting and guardrails. Much of the $80 million is directed toward highways washed out by heavy rains and flooding. DOT has provided a table listing the date, location, and amount of each emergency relief incident with this press release.
Source: http://www.dot.gov/affairs/dot11305.htm

11. *August 22, USA TODAY* — **Delta's future as stand−alone carrier in question.** A year ago, Delta Air Lines was struggling to stay out of bankruptcy−court protection. Increasingly, the question for the USA's No. 3 carrier, industry analysts say, is whether it can survive at all as an independent airline. Buckling under soaring fuel prices and $26 billion in debt, Delta got some relief last week when it sold a subsidiary, Atlantic Southeast Airlines, for $425 million. Delta executives now face a pivotal decision. They can stay the course and try to raise more cash by borrowing or by selling more assets. Or they can join competitors United Airlines and US Airways and attempt to reorganize in Chapter 11. Heavy debt, shrinking cash and a change in the law giving the airline more flexibility if it files before mid−October appear to be pushing it toward a bankruptcy filing. But in the world of $65−a−barrel oil and relentless low−fare competitors, Delta's historic strengths may not be enough to carry it beyond bankruptcy. US Airways, for example, has visited Chapter 11 twice since 2002 and couldn't survive alone. It's being acquired by America West. "As a stand−alone carrier, Delta is the weakest of the Big Five (American, United, Delta, Continental, Northwest)," says airline analyst Bill Warlick of Fitch Ratings, because it doesn't have as broad an international route network.
Source: http://www.usatoday.com/travel/news/2005−08−22−delta−cover_x .htm

[Return to top]

Postal and Shipping Sector

12. *August 16, News Sentinel (IN)* — **Post office gets biohazard system.** Fort Wayne is one of several Indiana cities receiving equipment to detect anthrax in the mail. Two Biohazard Detection Systems (BDS) should be operational by September 9 at the U.S. Postal Service’s processing and distribution center on Clinton St. Each costs about $150,000, paid for by a federal homeland security grant. Some 275,000 pieces of mail are sorted daily at the center, and about 236 employees work there during a 24−hour period. The machines will be operational 4−10 p.m., the center’s peak hours. In October 2001, two postal workers at the center that processes mail for Capitol Hill in Washington, DC, died after inhaling spores of anthrax, the same poison found on mail sent to several lawmakers there. The BDS system includes a hood, designed to suck in air particles, which will be installed on the current mail−processing equipment. Testing will be done hourly wherein air particles from the mail are placed in sterile water to make a liquid sample. The sample is then inserted into a cartridge for a DNA analysis.

If the test is positive for anthrax, a horn will sound, and employees will be evacuated.
Source: http://www.fortwayne.com/mld/fortwayne/news/local/12397018.h tm

[Return to top]

Agriculture Sector

13. *August 23, Wisconsin Ag Connection* — **New state animal ID law applies to all livestock owners.** The group that was founded to create a state−wide livestock identification database is reminding all livestock owners in Wisconsin that the new premises ID law scheduled to take effect this year applies to everyone. Wisconsin Livestock Identification Consortium COO Robert Fourdraine says registering premises is the first phase of a three−step national program to achieve a trace back system to identify all animals and premises potentially exposed to a foreign animal disease within 48 hours of discovery. "Premises registration is not aimed solely at traditional large scale agriculture," Fourdraine reminds producers. "Any person who keeps, houses, or co−mingles livestock as defined by law is subject to registering premises." Identifying all production points where livestock are raised and/or held is basic to developing a system able to respond to an animal disease outbreak. The new state law does not require anyone to participate in phase two of the plan, in which animals will be individually identified, or in some cases, identified by groups or lots. But phase one, called the Wisconsin Premises Registration Act, does take effect on November 1.
WLIC Website: http://www.wiid.org/
Source: http://www.wisconsinagconnection.com/story−state.cfm?Id=1009 &yr=2005

14. *August 23, Associated Press* — **Drought hurting cattle farmers.** Jessamine, KY, farmer Charles Miller usually doesn't start feeding hay to his cattle until the snow flies, but this year his 700 beef cattle have eaten hay for three weeks because of a summer drought. That has the Miller worried about hay supplies for winter. The dry spell threatens to squeeze profits for some cattle operators in Kentucky, the nation's top beef cattle producer east of the Mississippi River, with sales of $620.7 million last year. The drought could force some producers to cull herds to compensate for short hay supplies. Fellow cattle producer David Neville spent Monday, August 22, weighing calves that were weaned a month earlier than normal, also due to the drought. Neville said the calves' weight might be down as much as 20 percent, and he planned to feed them a special grain supplement to put on weight. "Every stage of production in the life of a cow−calf operation is affected by the drought," said Neville, a cattle producer in Shelby and Henry counties. Neville usually doesn't start supplying hay to his cows until Christmas, but expects to move up those feedings to late September because of poor pasture conditions.
Source: http://news.enquirer.com/apps/pbcs.dll/article?AID=/20050823/NEWS0103/508230344/1059/NEWS01

15. *August 23, Capital Press (OR)* — **Virus strikes onion fields.** Iris yellow spot virus is spreading in Southwest Idaho and Eastern Oregon onion fields this year. The disease began showing up fairly extensively throughout the entire Treasure Valley in late July, said Lynn Jensen, Oregon State University extension educator. The insect−born virus strikes and kills plant stalks, leaving fields a tangled mass of yellowed foliage. While it doesn't infect the bulbs, killing the tops robs the onions of their food source, halting their growth, said Krishna Mohan, University of Idaho

plant pathologist. Our onion trade is mostly based on the size of the bulb, he said. This disease affects the size, and that in turn affects the marketable yield.
Additional information about iris yellow spot virus:
http://www.apsnet.org/pd/searchnotes/2005/PD−89−0105C.asp
Source: http://www.capitalpress.info/main.asp?SectionID=67&SubSectionID=792&ArticleID=19306&TM=40707.52

16. *August 23, Casper Star Tribune (WY)* — **Wyoming will seek brucellosis−free status.** Nearly two years after losing it, Wyoming will seek to regain its federal brucellosis−free status in December, a task force working on brucellosis issues was told Monday, August 22. State Veterinarian Dwayne Oldham told members of the Wyoming Brucellosis Coordination Task Force that he wasn't sure of Wyoming's chances for regaining its brucellosis−free status. But Oldham said he hopes the recommendations and steps the state has taken in regard to solving its brucellosis problem will convince federal officials to reinstate the brucellosis−free designation. Many elk and bison in western Wyoming are infected with brucellosis, a livestock and wildlife disease that can cause cows, elk, and bison to abort their fetuses. Wyoming lost is brucellosis−free status in late November 2003. The loss came after the discovery that a cattle herd next to the Wyoming Game and Fish Department's Muddy Creek elk feedground near Pinedale was infected with the disease. The discovery caused several states, including Nebraska and Idaho, to enact restrictions on Wyoming cattle imports and led to costly testing of Wyoming cattle before they are sold. Increased surveillance across the state also turned up subsequent outbreaks of the disease in Teton and Washakie county cattle herds.
Source: http://www.casperstartribune.net/articles/2005/08/23/news/wyoming/b52ea45fbd21a65e8725706600063691.txt

17. *August 22, Pennsylvania Department of Agriculture* — **Group working to prevent the introduction of chronic wasting disease in Pennsylvania.** Agriculture Secretary Dennis Wolff Monday, August 22, outlined Pennsylvania's plan to prevent the introduction of chronic wasting disease (CWD) in the commonwealth. The CWD Response Plan, which addresses prevention, surveillance, response, and recovery activities, is a collaborate effort of the Pennsylvania Department of Agriculture (PDA), the Pennslvania Game Commission (PGC), U.S. Animal and Plant Health Inspection Service, and industry stakeholders. "Early detection is certainly the key to successful containment of CWD," said Wolff. "We are currently working with the task force to develop a mandatory surveillance requirement for Pennsylvania's captive cervid herds." At present, more than 250 herds participate in PDA's voluntary CWD Herd Certification Program. In addition, PDA provides laboratory testing, materials, and staff to assist the PGC with wild deer and elk CWD surveillance. This year, PGC plans to test at least 4,000 hunter−harvested wild deer for the disease.
PGC Website: http://www.pgc.state.pa.us/pgc/cwp/view.asp?A=458&QUESTION_ID=150496
PDA Website: http://www.agriculture.state.pa.us/agriculture/cwp/view.asp? q=127774
APHIS Website: http://www.aphis.usda.gov/vs/nahps/cwd/
Source: http://www.agriculture.state.pa.us/agriculture/cwp/view.asp? A=390&Q=135747

18. *August 22, Department of Homeland Security* — **Fact Sheet: National Bio and Agro−Defense Facility.** The Department of Homeland Security (DHS) is leading a requirements analysis process to identify a next−generation biological and agricultural defense facility to replace the

important but aging facility at Plum Island, New York. The Plum Island Animal Disease Center (PIADC) is an essential component of the national strategy for protecting U.S. agriculture from a bioterrorist attack involving the intentional introduction of foreign animal diseases such as foot−and−mouth disease, as described in the Homeland Security Presidential Directive, "Biodefense for the 21st Century." The President's FY06 budget requests $23 million for the needs assessment and design process for a new National Bio and Agro−defense Facility (NBAF). In addition to agricultural and animal studies, public health threats from emerging high consequence zoonotic pathogens and the development and licensure of medical countermeasures are generating additional demands for biocontainment laboratory space. DHS is working closely with the U. S. Department of Agriculture and the U.S. Department of Health and Human Services to evaluate future needs in the context of this new national facility. The options for a location, or locations, for the biocontaiment facilities have not been identified at this time, but will be considered during the conceptual design study.
Plum Island Animal Disease Center:
http://www.ars.usda.gov/main/site_main.htm?modecode=19400000
Source: http://www.dhs.gov/dhspublic/display?content=4752

[Return to top]

Food Sector

19. *August 22, Food Safety and Inspection Service* — **Ground beef patties recalled.** Flanders Provision Co., Inc., a Waycross, GA, establishment, is voluntarily recalling approximately 900,000 pounds of frozen ground beef patties that may be contaminated with E. coli O157:H7, the U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) announced Monday, August 22. The products were distributed to retail stores nationwide. The recall was initiated following a food safety assessment triggered by an FSIS epidemiological investigation. E. coli O157:H7 is a potentially deadly bacteria that can cause bloody diarrhea and dehydration.
Source: http://www.fsis.usda.gov/News_&_Events/Recall_033_2005_Relea se/index.asp

[Return to top]

Water Sector

20. *August 22, Associated Press* — **Water park illnesses grows.** New York state assemblyman Joseph Morelle is launching an inquiry into the state−run water playground that may have spread more than 2,000 cases of gastrointestinal illnesses. The number of reported gastrointestinal illnesses possibly spread by the water playground at Seneca Lake Park has grown to 2,202 cases across 24 counties in western and central New York as of Monday, August 22. So far, 13 cases in four different counties have been confirmed as cryptosporidiosis, a common waterborne disease. Tests conducted by the Health Department have found the presence of cryptosporidium in two storage tanks that supply water for the spray park.
Source: http://hosted.ap.org/dynamic/stories/B/BRF_SPRAYGROUND_ILLNE SSES?SITE=7219&SECTION=HOME&TEMPLATE=DEFAULT&CTIME=2005−08−2 2−19−19−32

[Return to top]

Public Health Sector

21. *August 23, Reuters* — **China's south on high alert as pig disease spreads.** China's far south is on high alert after one person was killed and three were infected by a pig−borne disease that has killed nearly 40 in the southwest, suggesting dangerous meat is being traded across the country. The latest victim of the disease, caused by the Streptococcus suis bacterium, had handled infected pork, Xinhua news agency said on Tuesday, August 23. The three infected patients, all butchers, also likely had contact with tainted meat. The central government said on Monday, August 22, it had the disease under control in Sichuan province, the epicenter of the outbreak and China's top pork−producing region. To contain the bacterium and other animal−borne diseases, China must focus more on animals, Henk Bekedam, a World Health Organization representative for China, told Reuters. "If you go to deal with human health issues only when it strikes people, I think you're already one step behind," Bekedam said. "You can never build a defense system if you only beef up the human side." Most of the more than 200 people who have contracted the pig−borne bacterium became sick after slaughtering, handling, or eating infected swine. The pig−borne disease first surfaced in Sichuan in June.
Additional information about Streptococcus suis is available from WHO:
http://www.wpro.who.int/health_topics/streptococcus_suis/
Source: http://today.reuters.com/news/newsArticle.aspx?type=worldNews&storyID=2005−08−23T114327Z_01_EIC342155_RTRIDST_0_INTERNATIONAL−CHINA−DC.XML

22. *August 23, Bloomberg* — **Indonesian polio cases rise.** Indonesia's polio cases rose to 225, with a fourth case reported in the capital Jakarta, a week before the nation holds its third vaccination campaign this year, the World Health Organization (WHO) said. The number includes a 25−year−old man who died in West Jakarta. There were four new cases in Banten province. More than 1,020 cases of polio, which causes paralysis and sometimes death and affects mainly children under five years old, have been confirmed in 13 countries this year. Indonesia plans to hold a nationwide vaccination campaign on August 30 and September 27 in all 33 provinces in the country to halt the spread of the disease, targeting 24.4 million children under five years old. Six countries are still polio−endemic: Afghanistan, Egypt, India, Niger, Nigeria, and Pakistan. Six other nations, all in Africa, are listed by WHO as having ``re−established transmission," with outbreaks lasting more than six months.
Global Polio Eradication Initiative: http://www.polioeradication.org/
Source: http://www.bloomberg.com/apps/news?pid=10000080&sid=a96kI2ISAQrA&refer=asia

23. *August 23, Reuters* — **Deadly bird flu strain confirmed in Kazakh villages.** A bird flu outbreak in seven northern Kazakh villages is dangerous to humans and threatening the west of the sprawling country, the Agriculture Ministry said on Tuesday, August 23. "The H5N1 strain has been detected in all seven villages," Asylbek Kozhumratov, director of the ministry's Veterinary Department, told reporters. "The western region is now in the risk zone because (migratory) birds are starting to fly to the Caspian Sea and Urals−Caspian basin," he said. The outbreak, which spread from Siberia in neighboring Russia, has prompted fears in Europe that the disease might spread there and unleash an influenza pandemic. Kozhumratov said no new

cases had been reported since August 15 in Kazakhstan, but that authorities would keep quarantines and other measures against bird flu in place until the end of October as a precaution. Since its discovery on a farm in Siberia in mid−July, bird flu has spread to other areas in Russia. More than 130,000 birds have been culled to try to prevent further contagion. Another 11,715 birds died of the virus, the Russian Emergencies Ministry said in a report on Tuesday, August 23. In Kazakhstan, at least 9,000 birds have died or been destroyed since the outbreak started in the north of the Central Asian state last month.
Source: http://www.alertnet.org/thenews/newsdesk/L23512204.htm

24. *August 23, BBC News* — **United Kingdom farmers in talks on bird flu.** United Kingdom (UK) Farmers' leaders are due to meet the government to discuss precautions against bird flu. The Department of Food, Environment and Rural Affairs (Defra) will aim to reassure farmers about current risks to the UK of the disease. Dutch farmers have been told not to keep birds outdoors amid concern that the disease may spread to Europe. The National Farmers' Union (NFU) wants to know if the decision not to adopt the ban in the UK will stay in force. Defra said Monday, August 22, that UK action similar to that in the Netherlands would be disproportionate, as the risk of the virus spreading to the UK was very low. The Dutch measures were put in place after an outbreak of bird flu was confirmed in Russia. Reports from the Russian government indicate the strain of bird flu is moving westward −− and is likely to reach Europe as birds migrate. The strain found in the Altai, Novosibirsk and Omsk regions has been identified as H5N1 −− the type that has killed at least 57 people in South−East Asia since 2003.
Defra Website: http://www.defra.gov.uk/
Source: http://news.bbc.co.uk/2/hi/uk_news/4176454.stm

[Return to top]

Government Sector

25. *August 23, The White House* — **President George W. Bush appoints Charles E. Allen to be Assistant Secretary for Information Analysis.** President George W. Bush on Tuesday, August 23, announced his intention to appoint Charles E. Allen, of North Carolina, to be Assistant Secretary for Information Analysis at the Department of Homeland Security. Allen currently serves as Special Assistant to the Director of the Central Intelligence Agency. He has served with the CIA since 1958. Prior to his appointment as Special Assistant, Allen served as Assistant Director of Intelligence for Collection. He also served as Chief of Intelligence in the CIA's Counterterrorist Center. Earlier in his career, Allen was assigned overseas in an intelligence liaison capacity. He received his bachelor's degree from the University of North Carolina at Chapel Hill.
Source: http://www.whitehouse.gov/news/releases/2005/08/20050823−2.h tml

[Return to top]

Emergency Services Sector

26.

August 23, The Daily Ardmoreite (OK) — **New technology to bring warnings to Oklahoma residents.** Armed with new cutting−edge technology called The Safe Community Alert Network (SCAN), the Marietta, OK, Emergency Management Agency (EMA) will soon begin sending public safety warnings and emergency alerts directly to the computers, mobile phones, personal data assistants (PDAs), pagers and fax machines of local residents. EMA director Tracey Smithwick said important alerts about sexual predators, neighborhood crime, local terrorist acts and Amber alerts will now reach community members in a matter of moments, no matter where they originate. This service is free, but residents must register at www.scanusa.com in order to receive the alerts. SCAN is the first national alert system that allows local public safety agencies to broadcast localized emergency information directly to the computers, mobile phones and PDAs of its citizens. Registered users can choose to receive any or all types of alerts to one or more of their digital information devices. Alert classifications include sexual predator, neighborhood crime, public safety, fire, traffic, public health, environmental, severe weather, cyber, Amber, Homeland Security and other miscellaneous warnings or emergencies. SCAN is available at no cost to public safety agencies or taxpayers.
SCAN USA: http://www.scanusa.com/
Source: http://ardmoreite.com/stories/082305/loc_0823050031.shtml

[Return to top]

Information Technology and Telecommunications Sector

27. *August 22, Secunia* — **ELM "Expires" header parsing buffer overflow vulnerability.** A vulnerability has been reported in ELM, which can be exploited by malicious people to compromise a user's system. The vulnerability is caused due to a boundary error when parsing the "Expires" header and can be exploited to cause a stack−based buffer overflow by sending a specially crafted e−mail to a user. Successful exploitation allows execution of arbitrary code. The vulnerability has been reported in versions 2.5 PL7, 2.5 PL6, and 2.5 PL5. Prior versions may also be affected. Users should update to version 2.5 PL8.
Source: http://secunia.com/advisories/16508/

28. *August 22, FrSIRT* — **AreaEdit "aspell_setup.php" remote code execution vulnerability.** A vulnerability was identified in AreaEdit, which may be exploited by remote attackers to execute arbitrary commands. This flaw is due to an input validation error in the "aspell_setup.php" script when handling a specially crafted "dictionary" parameter, which may be exploited by a remote attacker to cause arbitrary shell commands to be executed. AreaEdit versions prior to 0.4.3 are affected.
Users should upgrade to AreaEdit version 0.4.3:
http://www.formvista.com/otherprojects/areaedit.html
Source: http://www.frsirt.com/english/advisories/2005/1494

29. *August 22, Security Focus* — **PostNuke DL−viewdownload.PHP SQL injection vulnerability.** PostNuke is prone to an SQL injection vulnerability. This issue is due to a lack of sufficient sanitization of user−supplied input. Successful exploitation could result in a compromise of the application, disclosure or modification of data, or may permit an attacker to exploit vulnerabilities in the underlying database implementation. Security Focus is not aware of any vendor−supplied patches for this issue.

Source: http://www.securityfocus.com/bid/14636/info

30. *August 22, FrSIRT* — **BEA WebLogic Portal unauthorized remote access vulnerability.** A vulnerability was identified in BEA WebLogic Portal, which may be exploited by attackers to gain unauthorized access. This flaw occurs on Websites that use entitlements placed directly on desktop books, pages, or portlets, which could be exploited by remote attackers to access all the pages of the Book via specially crafted HTTP GET requests. No further details have been disclosed. Entitlements that are placed on Portals built from library books, pages, and portlets are not affected by this issue. Products affected are BEA Systems WebLogic Portal 8.1 SP1−SP4.
Patch for BEA WebLogic Portal 8.1 SP4:
ftp://ftpna.beasys.com/pub/releases/security/patch_CR238578_81SP4.zip
Source: http://www.frsirt.com/english/advisories/2005/1495

31. *August 22, FrSIRT* — **Cisco IDS Management Software SSL Certificate validation vulnerability.** A vulnerability was identified in CiscoWorks Management Center for IDS Sensors (IDSMC) and Monitoring Center for Security (Security Monitor or Secmon), which could be exploited by remote attackers to bypass the security restrictions. This flaw is due to an error in the SSL certificate checking functionality that does not properly validate SSL certificates, which could be exploited by attackers to spoof an IDS or IPS and then gather login credentials, submit false data, and filter legitimate data from. Products affected are IDSMC version 2.0 and 2.1, and CiscoWorks Monitoring Center for Security (Security Monitor or Secmon) version 1.1, 2.0 and 2.1.
This vulnerability has been addressed in Service Pack 1 for IPSMC 2.1 and Security Monitor 2.1: http://www.cisco.com/pcgi−bin/tablebuild.pl/mgmt−ctr−ids−app
Source: http://www.frsirt.com/english/advisories/2005/1497

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of a public exploit for a vulnerability in the Microsoft DDS Library Shape Control (msdds.dll) component, which comes with various Microsoft products such as Visual Studio .NET and Microsoft Office. Systems with Visual Studio .NET 2002, which installs msdds.dll version 7.0.9466.0, are vulnerable. Based on initial testing, msdds.dll version 7.10.3077.0 does not appear vulnerable. This version of the dll is installed with Office 2003 and Visual Studio .NET 2003. Although MS Office XP provides a vulnerable version of msdds.dll, it does not appear that IE will instantiate the COM object in question with the standard installation.

By convincing a user to view an HTML document (e.g., a web page or an HTML

email message) that attempts to instantiate the Microsoft DDS Library Shape Control COM object, a remote attacker could execute arbitrary code on the user's system with privileges of the user. More information about this vulnerability can be found in the following US−CERT Vulnerability Note:

VU#740372 − Microsoft DDS Library Shape Control (msdds.dll) COM object contains an unspecified vulnerability

This vulnerability has similar characteristics to the previously posted javaprxy.dll vulnerability (VU#939605). The underlying vulnerability is that Internet Explorer will instantiate non−ActiveX COM objects that are referenced in an HTML document. This can cause Internet Explorer to crash. More information about this vulnerability can be found in the following US−CERT Vulnerability Note:

VU#680526 − Microsoft Internet Explorer allows non−ActiveX COM objects to be instantiated

Until a patch is available to address this vulnerability, US−CERT strongly encourages users to review the workarounds section of Vulnerability Note (VU#740372). Additionally, Microsoft has published a Security Advisory about this issue and is continuing to investigate the problem.

Current Port Attacks

Top 10 Target Ports	445 (microsoft−ds), 1026 (−−−), 6881 (bittorrent), 1433 (ms−sql−s), 135 (epmap), 80 (www), 139 (netbios−ssn), 1434 (ms−sql−m), 50000 (SubSARI), 4672 (eMule) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

32. *August 22, The Register (UK)* — **Vulnerabilities found in hotel broadband systems.** Hotel hybrid broadband Internet and TV−on−demand entertainment systems are open to attack, security researchers warn. Penetration testing firm SecureTest has identified a number of vulnerabilities in the implementation of hotel broadband systems delivered using Cisco's LRE (long−reach Ethernet) technology. Using a laptop connected to a hotel network, SecureTest found it was possible to control the TV streams sent to each room or gain access to other user’s laptops. According to SecureTest, a hacker might be able to access this menu and configure the system to broadcast content directly from a laptop over the TV. In theory, this could enable hackers to download and broadcast any material throughout the hotel complex. "A hacker or disgruntled employee could get their kicks by accessing and manipulating the TV menu, but this breach has much wider implications. An individual could broadcast their own advertising or an activist their own political message to every room," said Ken Munro, managing director

of SecureTest. "Moreover, fixed Internet access is inadequately protected in many cases. People plug into a hotel network assuming it's a trusted connection but it's not. Unless they have a personal firewall running, fraudsters can snoop on desktops at leisure."
Source: http://www.theregister.co.uk/2005/08/22/hotel_hacking_reload ed/

[Return to top]

General Sector

Nothing to report.
[Return to top]